

SBA PRIVACY IMPACT ASSESSMENT

**Freedom of Information/Privacy Acts Office & Office of the Chief Information Officer
Small Business Administration
409 3rd Street, S.W.
Washington, DC 20416**

Hearings & Appeals Case Tracking System (OHACTS)

June, 2004

Revision Sheet

| Release No. | Date | Revision Description |
|-------------|------------|----------------------|
| 1.0 | June, 2004 | Privacy Assessment |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

**Privacy Impact Assessment Authorization
Memorandum**

I have carefully assessed the Privacy Impact Assessment for the Freedom of Information/Privacy Acts Case Tracking System. This document has been completed in accordance with the requirements of the SBA System Development Methodology.

MANAGEMENT CERTIFICATION - Please check the appropriate statement.

_____ The document is accepted.

_____ The document is accepted pending the changes noted.

_____ The document is not accepted.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

Project Leader
Barbara S. Brown

DATE

Program Area/Sponsor Representative
Samantha Y. Wiggins

DATE

Program Area/Sponsor Director
Delorice P. Ford

DATE

TABLE OF CONTENTS

1.0 INTRODUCTION AND OVERVIEW 1
1.1 Background 1
1.2 The Freedom of Information/Privacy Acts Office 1
1.3 Privacy Impact Assessment 2
2.0 PRIVACY ISSUES IN INFORMATION SYSTEMS 3
2.1 Privacy Act of 1974 5 U.S.C. 552a As Amended..... 3
2.2 Definitions:..... 4
2.3 Information and Privacy..... 4
2.4 Data in the System 5
2.5 Access to the Data..... 5
2.6 Attributes of the Data 5
2.7 Maintenance of Administrative Controls 5
3.0 PRIVACY ASSESSMENT 6
3.2 Access to the Data..... 7
3.3 Attributes of the Data 9
3.4 Maintenance of Administrative Controls 10
APPENDIX A..... 5

1.0 INTRODUCTION AND OVERVIEW

1.1 Background

The Small Business Administration is responsible for ensuring the privacy, confidentiality, integrity, and availability of client and employee information. The SBA recognizes that privacy protection is both a personal and fundamental right of all clients, partners, and employees. Among the most basic of clients, partners, and employees' rights is an expectation that the SBA will protect the confidentiality of personal, financial, and employment information. Clients, partners, and employees also have the right to expect that the SBA will collect, maintain, use, and disseminate identifiable personal information and data only as authorized by law and as necessary to carry out agency responsibilities. Client and employee information is protected by the following:

- Privacy Act of 1974, as Amended (5 USC 552a) which affords individuals the right to privacy in records that are maintained and used by Federal agencies. Note that 5 USC 552a includes the Computer Matching and Privacy Act of 1988 (Public Law 100-503);
- Computer Security Act of 1987 (Public Law 100-235) which establishes minimum security practices for Federal computer systems;
- 13 CFR 102.20 Privacy Act Regulations;
- OMB Circular A-130, Management of Federal Information Resources, which provides instructions to Federal agencies on how to comply with the fair information practices and security requirements for operating automated information systems;
- OMB Circular A-11, Part 7: Planning, Budgeting, Acquisition and Management of Capital Assets, which prescribes how security and privacy safeguards should be treated in agencies' capital plans for major information technology projects. (Circular A-11 is re-issued annually)
- Freedom of Information Act, as Amended (5 USC 552) which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.

1.2 The Freedom of Information/Privacy Acts Office

The Freedom of Information/Privacy Acts Office is the SBA organization responsible for managing SBA's appellate function, as well as developing the Agency's policy and procedures regarding the FOI/PA. Besides the FOIA duties, the Office is responsible for: ensuring that the Agency adheres to requirements of the PA and maintains administrative control of SBA activities implementing the act; decides all administrative PA appeals; educates SBA components about their PA responsibilities, and advises Agency personnel, clients of the Agency and the general public regarding all aspects of the Act; prepares the Biennial Privacy Act Report to OMB.

1.3 Privacy Impact Assessment

The Privacy Impact Assessment is a process used to evaluate privacy in information systems. The process is designed to guide system owners and developers in assessing privacy through the early stages of development. The process consists of privacy training, gathering data on privacy issues from the project, identifying and resolving any privacy risks, and approval by the Senior PA Officer. The PIA process is described in detail in Section III, Completing a Privacy Impact Assessment.

2.0 PRIVACY ISSUES IN INFORMATION SYSTEMS

2.1 Privacy Act of 1974 5 U.S.C. 552a as Amended

The Privacy Act of 1974 5 U.S.C. 552a As Amended requires Federal Agencies to protect personally identifiable information. It states specifically:

"each agency that maintains a system of records shall - "

- "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;"
- "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individuals rights, benefits, and privileges under Federal programs;"
- "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;"
- "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

2.2 Definitions:

Accuracy - within sufficient tolerance for error to assure the quality of the record in terms of its use in making a determination.

Completeness - all elements necessary for making a determination are present before such determination is made.

Determination - any decision affecting an individual which, in whole or in part, is based on information contained in the record and which is made by any person or agency.

Necessary - a threshold of need for an element of information greater than mere relevance and utility.

Record - any item, collection or grouping of information about an individual and identifiable to that individual that is maintained by an agency.

Relevance - limitation to only those elements of information which clearly bear on the determination(s) for which the records are intended.

Routine Use - with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

System of Records - a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual

2.3 Information and Privacy

To fulfill the commitment of the SBA to protect personal data several issues must be addressed with respect to privacy.

- The use of information must be controlled.
- Information may be used only for a necessary and lawful purpose.
- Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them.
- Information collected for a particular purpose should not be used for another purpose without the data subjects consent unless such other uses are specifically authorized or mandated by law.
- Any information used must be sufficiently accurate, relevant, timely and complete to assure fair treatment of the individual.

Given the availability of vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the SBA, to share that information. With the potential expanded uses of data in automated systems it is important to remember that information can only be used for the purpose for which it was collected unless other uses are specifically authorized or mandated by law. If the data is to be used for other purposes, then the public must be provided notice of those other uses.

These procedures do not in themselves create any legal rights, but are intended to express the full and sincere commitment of the SBA to the laws which protect client and employee privacy rights and which provide redress for violations of those rights.

2.4 Data in the System

The sources of the information in the system are an important privacy consideration if the data is gathered from other than SBA records. Information collected from non-SBA sources should be verified, to the extent practicable, for accuracy, that the information is current, and the information is complete. This is especially important if the information will be used to make determinations about individuals.

2.5 Access to the Data

Who has access to the data in a system must be defined and documented. Users of the data can be individuals, other systems, and other agencies. Individuals who have access to the data can be system users, system administrators, system owners, managers, and developers. When individuals are granted access to a system, their access should be limited, where possible, to only that data needed to perform their assigned duties. If individuals are granted access to all of the data in a system, procedures need to be in place to deter and detect browsing and unauthorized access. Other systems are any programs or projects that interface with the system and have access to the data. Other agencies can be International, Federal, state, or local entities that have access to SBA data.

2.6 Attributes of the Data

When requirements for the data to be used in the system are being determined, those requirements must include the privacy attributes of the data. The privacy attributes are derived from the legal requirements imposed by the Privacy Act of 1974. First, the data must be *relevant* and *necessary* to accomplish the purpose of the system. Second, the data must be *complete*, *accurate* and *timely*. It is important to ensure the data has these privacy attributes in order to assure fairness to the individual in making decisions based on the data.

2.7 Maintenance of Administrative Controls

Automation of systems can lead to the consolidation of processes, data, and the controls in place to protect the data. When administrative controls are consolidated, they should be evaluated so that all necessary controls remain in place to the degree necessary to continue to control access to and use of the data.

Data retention procedures should be documented. Data retention procedures require review to ensure they meet statutory and/or IRM requirements. Precise rules must be established for the length of time information is kept and for assuring that it is properly eliminated at the end of that time.

The intended and potential monitoring capabilities of a system must be defined and safeguards must be installed to ensure the privacy of clients and partners and prevent unnecessary intrusion. The use of monitoring capabilities should be limited, at a minimum, to some judicially ascertainable standard of reasonableness in light of the statutory mission of the SBA and other authorized governmental users of the system.

SECTION V PRIVACY QUESTIONS

3.0 PRIVACY ASSESSMENT

The OHA Case Tracking System (OHACTS) was developed for use by the Office of Hearings Appeals for tracking cases and appeals in a number of jurisdictional areas. The major application is used primarily by the clerks, attorneys, and judges.

3.1 Data in the System

1. Generally describe the information to be used in the system in each of the following categories: Citizen, Client/Partner, Employee, Other.

Litigant and or Business names, case description, date filed, date assigned, judge, agency, and agency contact information

2. What are the sources of the information in the system?

Appeals of determinations of proposed Agency actions.

- a. What SBA files and databases are used?

Sybase database, Web-enable system.

- b. What Federal Agencies are providing data for use in the system?

None

- c. What State and Local Agencies are providing data for use in the system?

None

- d. What other third party sources will data be collected from?

None

- e. What information will be collected from the client/partner/employee?

Litigant and or Business names, address, telephone and fax numbers

3. a. How will data collected from sources other than SBA records and the partner or client be verified for accuracy?

N/A

b. How will data be checked for completeness?

N/A

c. Is the data current? How do you know?

N/A

4. Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes, OHA Physical Data Dictionary.xls

Access to the Data

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?

Hearing & Appeals staff, systems developers, and database support personnel.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Security roles have been defined based on the roles of the existing user community. SBA's IT security team will be responsible for granting access to OHA CTS at the appropriate security level using the Security System.

3. Will users have access to all data on the system or will the users' access be restricted?

No, user access will be restricted.

Read Only (ATTORNEY)

The attorney will have the ability to generate reports and view all information about the case including the judge's comments.

This role cannot access the Code Maintenance module and has no update capability.

UPDATE Only (CLERK)

The clerk has the ability to enter all information pertaining to a case and generate reports.

The clerk also has the ability to modify all case information, with the exception of judge comments.

This role cannot access the Code Maintenance module.

UPDATE Only (JUDGE)

The judge has the ability to review and update individual case information, and generate reports.

This role cannot modify case information or access the Code Maintenance module.

UPDATE Only (SYSTEM ADMINISTRATOR)

The Administrator can generate reports, as well as enter and modify all case information with the exception of judge comments.

The Administrator has exclusive access to the Code Maintenance module.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?

Security roles, userid, and password.

5. a. Do other systems share data or have access to data in this system? If yes, explain.

No

- b. Who will be responsible for protecting the privacy rights of the citizens, partners, clients, and employees affected by the interface?

N/A

6. a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?

No

- b. How will the data be used by the Agency?

N/A

c. Who is responsible for assuring proper use of the data?

N/A

d. How will the system ensure that agencies only get the information they are entitled to under 13 CFR 102.20?

N/A

Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes

2. a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No

b. Will the new data be placed in the individual's record (citizen, client, partner, or employee)?

N/A

c. Can the system make determinations about citizens, clients, partners, or employees that would not be possible without the new data?

N/A

d. How will the new data be verified for relevance and accuracy?

N/A

3. a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

N/A

b. If processes are being consolidated, will the proper controls remain to protect the data and prevent unauthorized access? Explain.

N/A

4. a. How will the data be retrieved?
Litigant and/or Business names, *Case* type, date filed

Can it be retrieved by personal identifier?

Litigant and/or Business names

- b. What are the potential effects on the due process rights of citizens, clients, partners, and employees of:

| | | |
|---|---|-----|
| ? | consolidation and linkage of files and systems; | N/A |
| ? | derivation of data; | N/A |
| ? | accelerated information processing and decision making; | N/A |
| ? | use of new technologies. | N/A |

How are those effects to be mitigated?

N/A

Maintenance of Administrative Controls

1. a. Explain how the system and its use will ensure equitable treatment of citizens, clients, partners and employees.

N/A

- b. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

OCIO database, system support, and OCIO web server support personnel will maintain system.

- c. Explain any possibility of disparate treatment of individuals or groups.

N/A

2. a. What are the retention periods of data in this system?

National Archives Records Administration Retention Schedules (060)

- b. What are the procedures for eliminating the data at the end of the retention period?
Where are the procedures documented?

The maintenance and disposition of records pertaining to the administration of the Privacy Act are outlined in General Records Schedule (GRS) 14

- c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

N/A

3. a. Is the system using technologies in ways that the SBA has not previously employed (e.g., Caller-ID)?

No

- b. How does the use of this technology affect citizen/client/partner/employee privacy?

N/A

4. a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Yes, employees' user ids and names and client's names will be displayed.

- b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

No

- c. What controls will be used to prevent unauthorized monitoring?

Access and use will be limited to the Office of Hearings & Appeals staff only and will require a user id.

5. a. Under which Systems of Record notice (SOR) does the system operate?

SBA 060 Grievances and Appeals

- b. If the system is being modified, will the SOR require amendment or revision? Explain.

N/A